IN THE UNITED STATES DISTRICT COURT
FOR NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE CELLULAR DEVICES ASSIGNED CALL NUMBERS (571) 201-1240, (774) 417-7789, AND (978) 815-1897, THAT IS STORED AT PREMISES CONTROLLED BY T-MOBILE AND SPRINT	Case No. 18-mj-275, 276, 277 -01-AJ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANTS

I, Joseph T. Gugliotta, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for three search warrants for (i) information associated with certain cellular telephones assigned call numbers **(571) 201-1240** and **(774) 417-7789**, that are stored at premises controlled by T-Mobile, a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, NJ 07054 (the "T-MOBILE PHONES") and (ii) information associated with a certain cellular telephone assigned call number **(978) 815-1897**, that is stored at premises controlled by Sprint, a wireless telephone service provider headquartered at 6200 Sprint Parkway, Overland Park, KS 66251 (the "SPRINT PHONE"), collectively the "SUBJECT PHONES." The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for three search warrants under 18 U.S.C. § 2703(c)(1)(A) to require T-Mobile and Sprint to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of

Attachment B. This court has authority to issue this warrant under 18 U.S.C. §§ 2703(c)(1)(A), 2711(3)(A).

2. I am a U.S. Postal Inspector with the United States Postal Inspection Service (USPIS) and have been since 2006. I am assigned to the USPIS Boston Division where I am a member of the Mail Theft and Identity Theft Team, which investigates, among other things, financial crimes involving mail theft and the theft of personal identifiers and financial account numbers. During my employment as a U.S. Postal Inspector, I have conducted and participated in investigations of numerous financial crimes involving mail, bank, and wire fraud, as well as identity theft, money laundering, and counterfeit financial instruments. I have served as the affiant on search warrants.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that the following crimes have been committed, are being committed, and will be committed by Nicholas MEALEY, Darcy MORANDI, Roland HOLLENBECK, and other unknown persons: Aggravated Identity Theft, in violation of 18 U.S.C. § 1028A; Access Device Fraud in violation of 18 U.S.C. § 1029; Bank Fraud, in violation of 18 U.S.C. § 1344; Conspiracy to Commit Bank Fraud in violation of 18 U.S.C. § 1349; and Conspiracy to Commit Offense or Defraud United States, in violation of 18 U.S.C § 371. There is also probable cause to search the information described in Attachment A for evidence or instrumentalities of these crimes as further described in Attachment B.

PROBABLE CAUSE

5. Since on or about January 20, 2018, agents from the United States Postal Inspection Service ("USPIS") and the United States Secret Service ("USSS") have been conducting an investigation into debit card fraud associated with "skimmers" placed in gas pumps located at a VERC Gulf station located in Lynnfield, Massachusetts by presently unknown individuals (the "VERC Skimmers"). The skimmers copy information from debit and credit cards used at the gas station. Through my investigation, I have identified several known and unknown individuals who have used information obtained from the VERC Skimmers to make fraudulent purchases and ATM withdrawals in New Hampshire and Massachusetts with "cloned" debit cards that contain the stolen information.

6. Through my training and experience, I have learned that "skimmers" are a type of credit and debit card reader that can be disguised to look like part of an ATM or other card reading machine, placed inside the card reader slot, or installed inside the machine. Once inserted or installed, the skimmer can read and save credit and debit card information when individuals use the compromised machine. The card information can be retrieved from the skimmer, sometimes using wireless technology such as Bluetooth. This information can then be used for various forms of credit and debit card fraud such as making fraudulent purchases, withdrawing money from cardholders' accounts, or making counterfeit "cloned" credit and debit cards.

7. On January 20, 2018, R.P. called the Norwood, Massachusetts post office and reported she received notification that her debit card was used to purchase a Postal Money Order that she did not purchase and that her debit card was still in her possession. I contacted R.P. and

learned that her debit card was also used at a CVS in Foxboro, Massachusetts to make several large cash withdrawals. R.P. also told me she banks with Eastern Bank.

8. I contacted Eastern Bank and learned that R.P. and other Eastern Bank customers had used their debit cards at a VERC Gulf Station in Lynnfield, Massachusetts prior to their debit cards being used fraudulently. I also received reports from other banks of customers that had reported debit card fraud. I identified which cards were used at the VERC Gulf gas station in Lynnfield, Massachusetts prior to the fraudulent transactions.

9. On or about April 28, 2018, I received a Lynnfield Police Department report written by an officer who responded to a report of suspicious activity at the VERC Gulf gas station on December 10, 2017. According to this report, an employee of the gas station witnessed a silver vehicle parked at one of the pumps. When the employee pulled into the gas station at or about 4:50 a.m., she determined there were two men inside of the vehicle and a third man standing by one of the gas pumps, which had been opened. When the employee confronted the individuals, the vehicle fled the scene. A subsequent investigation by responding officers revealed all ten gas pumps had been opened such that one could access to the section of the pump where an internal skimmer could be installed or retrieved. However, no skimmers were found.

10. On March 1, 2018, Special Agent Jessica Brannan, USSS, and I inspected all of the gas pumps with a technician who services the pumps. We did not find skimming devices.

11. On March 14, 2018, I received a report that a technician servicing the pumps at the VERC Gulf station discovered two Bluetooth-enabled gas pump skimmers. Special Agent Brannan and I responded to the VERC Gulf station and seized the skimming devices.

12. In my training and experience, a Bluetooth-enabled skimmer allows individuals to download skimmed debit and credit card information wirelessly onto their computers or cellular devices.

13. Through my investigation, I have identified at least three groups of individuals that have used debit card information obtained from cards compromised by the VERC Skimmers to fraudulently withdraw money from ATMs and/or purchase, or attempt to purchase, postal money orders.

Group One (Victim: M.M.)

14. According to Eastern Bank records, on January 8, 2018, M.M. used his debit card at the VERC Gulf Station in Lynnfield, Massachusetts. On January 23 and 24, 2018, R.M.'s debit card was used fraudulently at various locations in New Hampshire.

15. I interviewed M.M. on October 12, 2018. M.M. recalled frequently using his debit card at a gas station after the Christmas Tree Shop on Route 1 in the Lynnfield/Saugus area. According to Google Maps, this Christmas Tree Shop is located one-tenth of a mile from the VERC Gulf Station.

16. M.M. told me that he received an automated call from Eastern Bank reporting the possible fraudulent use of his debit card. He checked his account online, saw the fraudulent charges, and contacted Eastern Bank to report the fraud. M.M. recalled his debit card was fraudulently used at a CVS in New Hampshire. M.M. also recalled his compromised debit card was in his possession at the time of the fraudulent transactions.

17. Eastern Bank records indicate M.M's card was used at the locations charged below on January 23 and 24, 2018.

Date; Approx. Time	Location and Type of Transaction
1/23/2018; 12:44 p.m. to 12:47 p.m.	Rite Aid ATM withdrawal in Pelham, New Hampshire
1/23/2018; 2:15 p.m. to 2:24 p.m.	CVS attempted ATM withdrawal in Manchester, New Hampshire
1/23/2018; 3:05 p.m.	Attempted purchase of a money order at U.S. Post Office in Nashua, New Hampshire
1/24/2018; 11:32 to 11:34 a.m.	CVS attempted ATM balance inquiry in Sudbury, Massachusetts

18. I reviewed surveillance video from the dates and times of the transactions at the CVS in Manchester, NH and the CVS in Sudbury, Massachusetts. Based on my review of the CVS surveillance video from Manchester, New Hampshire and Sudbury, Massachusetts, the same three individuals worked in concert to fraudulently use M.M.'s debit card in New Hampshire and Massachusetts.

19. Footage at both locations shows a red vehicle park in the respective CVS parking lots. In the space of approximately 15 minutes, three individuals—two males and one female—separately and sequentially exit the vehicle and use the ATM. The individuals appear to be the same in each video.

20. According to Google Maps, the Nashua Post Office is 19.3 miles or a 25 minute drive from the CVS in Manchester. It is therefore probable that the same three individuals that used M.M.'s identity and debit card in Manchester at 2:24 pm on January 23, 2018, also used R.M.'s identity and debit card in Nashua at 3:05 pm that same day.

Group Two (Victims: C.B.)

21. According to a Winchester Savings Bank investigator, on February 21, 2018, C.B. used her debit card at the VERC Gulf Station in Lynnfield, Massachusetts. On March 1, 2018, C.B.'s debit card was used fraudulently at the Athol Savings Bank ATM in Ashburnham, Massachusetts, and at the CVS in Groton, MA.

22. I interviewed C.B. on October 11, 2018. She confirmed although she had possession of her debit card, she did not make the purchases described below in paragraphs 22 through 24 and 26.

23. Based on my review of Winchester Savings Bank and Athol Savings Bank records and surveillance video, as well as information provided to me by investigators at these banks, a white sedan with a black grill dropped off a man, later identified by local law enforcement as Roland HOLLENBECK, wearing a dark colored hooded sweatshirt with the text "Los Angeles" and a Nike Air Jordan logo at the drive-up Athol Savings Bank ATM machine at approximately 4:14 p.m. Athol ATM video shows HOLLENBECK with several cards with magnetic strips in his hand at the ATM. After he used the ATM, HOLLENBECK walked away from the ATM at approximately 4:17 p.m. and, according to the Athol Savings Bank investigator, got in the passenger side of the white sedan with the black grill, and drove away. The Athol ATM video shows HOLLENBECK wearing gray sweatpants and gray sneakers with black trim. I also observed nautical markings on the back of the sleeves of HOLLENBECK's sweatshirt.

24. According to Winchester Savings Bank records, C.B.'s debit card was used at 4:17 p.m.

25. Detectives from Ashburnham Police Department identified HOLLENBECK in the Athol ATM footage. The Ashburnham Police Department also interviewed HOLLENBECK's mother, who said she was 75% sure that the individual in the Athol ATM footage was her son, HOLLENBECK.

26. On May 7, 2018, I interviewed HOLLENBECK, who denied his involvement in the fraudulent transactions. He also told me that his personal cell phone was lost or damaged and

currently uses and carries his work cellphone as if it was his own phone, with a Sprint telephone number [redacted][1]

27. Winchester Savings Bank records also indicated C.B.'s debit card was fraudulently used at the CVS in Groton, MA on March 1, 2018 at 1:34 p.m. Based on my review of CVS surveillance video from the Groton location, a male individual wearing the same sweatshirt, sweatpants, and sneakers as HOLLENBECK in the Athol ATM video, entered the CVS in Groton at approximately 1:31 p.m. and left at 1:35 p.m.

Group Three (Victim: S.R.)

28. According to TD bank records, S.R., a resident of Peabody, Massachusetts, used his TD debit card at the VERC Gulf in Lynnfield, Massachusetts on January 25, 2018.

29. On or about March 17, 2018, I learned that S.R. reported his TD debit card was fraudulently used to buy Postal Money orders and to make ATM withdrawals. I interviewed S.R. on May 22, 2018, and October 9, 2018. He confirmed that he had purchased gas at the VERC station in the past, and, although he had possession of his debit card, he did not make the purchases described below in paragraphs 29 and 30.

30. The Peabody Police reported that S.R.'s debit card was used to withdraw money from an ATM at the BayCoast Bank in Fall River, Massachusetts on March 2, 2018 at 1:25 p.m.

31. Peabody Police Department provided me with BayCoast Bank ATM records and surveillance video incident to the use of S.R.'s debit card on March 2, 2018. I reviewed this surveillance video and saw that, prior to the fraudulent debit card transaction, a black Ford Focus

[1] Hollenbek's employer and the owner and account holder of the SPRINT PHONE, [redacted] in Gloucester, MA, has given written consent to Sprint to release the information sought by this warrant, including historic cell site information. In an abundance of caution, and at Sprint's request, I am seeking a search warrant for these records.

with Massachusetts license plate [redacted] pulled into the BayCoast Bank parking lot. A male exited from the front passenger side of the vehicle, pulled up the hood of his sweatshirt, entered the bank, and made an ATM withdrawal, removing the cash from the machine at or about 1:25 p.m. This male then exited the bank, entered the same Ford Focus on the front passenger side, and the vehicle left the bank parking lot.

32. I searched Massachusetts Vehicle Registration records and learned that the black Ford Focus with Massachusetts license plate [redacted] is registered to Nicholas MEALEY, [redacted] Massachusetts.

33. On June 15, 2018, Special Agent Brannan and I interviewed MEALEY at his [redacted] assachusetts address. MEALEY confirmed his phone number is [redacted] and told us he has had this number for three years. MEALEY also looked at the still photo of the black Ford Focus with Massachusetts license plate [redacted] which was derived from the BayCoast Bank video, and confirmed it was his vehicle.

34. MEALEY told us he frequently loans his car to his friend, "Darcy," and told us Darcy's phone number is [redacted]. Through my investigation, I have identified "Darcy" as Darcy MORANDI. MEALEY initially claimed difficulty recalling his whereabouts on March 2, 2018, and looked through the text messages on his cell phone to assist in his recollection. When he reached the text messages from March 2, 2018, the day S.R.'s debit card was used fraudulently, MEALEY voluntarily showed us a thread of text messages between him and MORANDI that supported his recollection that he dropped off his vehicle to MORANDI at MORANDI's house on that date for him to use.

35. According to the text messages on MEALEY's phone, MEALEY texted MORANDI at 10:48 a.m. and told him he arrived at MORANDI's house at 10:15 a.m. At 1:16

p.m., MEALEY received a text from MORANDI saying "worst case scenario just try to get out early enough so we can get up there before 9 cuz I'll definitely have the money to go tonight."

36. Between 3:06 p.m. and 3:23 p.m., MEALEY received a string of text messages from MORANDI indicating his progress in traveling to return MEALEY's car.

37. At 3:27 p.m., MEALEY received a text message from MORANDI stating "here." Although MEALEY denied any involvement with the BayCoast Bank transaction, MEALEY appeared extremely nervous while he perused his text messages to the point where his hands began to shake noticeably and he perspired heavily. MEALEY also appeared to conceal his phone from investigators' view unless the messages pertained specifically to the times his vehicle was being driven. In my training and experience, this behavior indicate that the person may not be completely forthcoming and may be trying to conceal something.

38. Based on my training an experience, I also know that members of a criminal conspiracy often use their cell phones to coordinate their activities and to communicate with each other. I also know that members of a conspiracy enter the conspiracy at different times, have different roles in the conspiracy, and who benefit in different ways from being in the conspiracy.

39. Based on the timeline established by MEALEY and MORANDI's text messages, I know that MORANDI borrowed MEALEY's vehicle from on or about 11:09 a.m. and returned it on or about 3:27 p.m. on March 2, 2018. According to Google Maps, the BayCoast Bank location where S.R.'s debit card was used is 1.8 miles or an 8 minute drive from MORANDI's residence.

40. There is probable cause that cell phone location information of the SUBJECT PHONES will verify and provide additional evidence regarding the activities of MEALEY, MORANDI, and HOLLENBECK when the fraudulent ATM transactions occurred. For

example, location information may assist in (i) confirming the locations of MEALEY, MORANDI and HOLLENBECK at the time of the fraudulent transactions; (ii) identifying other co-conspirators; (iii) providing evidence that MEALEY, MORANDI, and HOLLENBECK made fraudulent transactions at other locations unknown to investigators, or (iv) coordinated criminal activities with other coconspirators at locations unknown to investigators.

41. I also know that cell phones communicate with cell towers as the devices and their owners travel from one cell tower's coverage area to another. Knowing the location of the SUBJECT PHONES, as well as the items listed in Attachment B, therefore, will, among other things, assist me and Special Agent Brannan in determining the proximity of MEALEY, MORANDI, and HOLLENBECK vis-à-vis the locations where the skimmers were installed and where the fraudulent transactions took place in New Hampshire and Massachusetts. This information will also assist us in identifying other coconspirators.

42. In my training and experience, I have learned that T-Mobile and Sprint are companies that provide cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular

telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

43. Based on my training and experience, I know that T-Mobile and Sprint can collect cell-site data about the SUBJECT PHONES. I also know that wireless providers such as T-Mobile and Sprint typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

44. Based on my training and experience, I know that wireless providers such as T-Mobile and Sprint typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers such as T-Mobile and Sprint typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the SUBJECT PHONES' user or users and may assist in the identification of co-conspirators and/or victims.

AUTHORIZATION REQUEST

45. Based on the foregoing, I request that the Court issue the proposed search warrants, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

46. I further request that the Court direct T-Mobile and Sprint to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrants will be served on T-Mobile and Sprint, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

47. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed for one year. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

Respectfully submitted,

/s/ Joseph T. Gugliotta
Joseph T. Gugliotta
U.S. Postal Inspector
US Postal Inspection Service

Subscribed and sworn to before me on December 21, 2018.

/s/ Daniel J. Lynch
Hon. Daniel J. Lynch
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number **(571) 201-1240** that is stored at premises controlled by T-Mobile ("the Provider"), headquartered at 4 Sylvan Way, Parsippany, NJ 07054.

ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number **(774) 417-7789** that is stored at premises controlled by T-Mobile ("the Provider"), headquartered at 4 Sylvan Way, Parsippany, NJ 07054.

ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number **(978) 815-1897** that is stored at premises controlled by Sprint ("the Provider"), headquartered at 6200 Sprint Parkway, Overland Park, KS 66251.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period of on or about December 1, 2017 to December 21, 2018:

a. The following information about the customers or subscribers of the Account:

i. Names (including subscriber names, user names, and screen names);

ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

iii. Local and long distance telephone connection records;

iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

v. Length of service (including start date) and types of service utilized;

vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:

i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

ii. information regarding the cell tower and antenna face (also known as "sectors") through which the communications were sent and received.

iii. "per call measurement data" or any other data that estimates the distance of the cellular device from the cell tower.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence and instrumentalities of violations of 18 U.S.C. § 1028A, Aggravated Identity Theft; 18 U.S.C. § 1029, Access Device Fraud; 18 U.S.C. § 1344, Bank Fraud; 18 U.S.C. § 1349, Conspiracy to Commit Bank Fraud; and 18 U.S.C § 371, Conspiracy to Commit Offense or Defraud United States, involving Nicholas MEALEY, Darcy MORANDI, and Roland HOLLENBECK during the period of on or about December 1, 2017 to December 21, 2018.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by T-Mobile, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of T-Mobile. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of T-Mobile, and they were made by T-Mobile as a regular practice; and

b. such records were generated by T-Mobile electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of T-Mobile in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by T-Mobile, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Sprint, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Sprint. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Sprint, and they were made by Sprint as a regular practice; and

b. such records were generated by Sprint electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Sprint in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Sprint, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature